

ИСТОРИЯ РАЗВИТИЯ ШИФРУЮЩЕЙ АППАРАТУРЫ В РОССИИ



Появление средств электросвязи во второй половине XIX века и их бурное развитие в XX веке открыло перед человечеством новые возможности для повышения оперативности связи и поставило ряд трудных и принципиально новых задач в разработке аппаратуры скрытия передаваемой информации. Использование ручных шифров и

машин предварительного шифрования, особенно при ведении переговоров по каналу связи, становится явно нецелесообразным. Нужно было привести время шифрования на передаче и приеме в соответствие с практически мгновенной скоростью передачи информации по каналам связи.

5 мая 1921 года декретом Совнаркома создается специальная служба для решения общих вопросов организации в стране секретной связи, разработки государственных шифров, рекомендаций по их использованию и осуществления контроля над правильным их применением.

Телефонная связь является наиболее оперативной и удобной для абонентов и дает возможность с малой затратой времени обсуждать и решить необходимые для них вопросы.

Проблема линейного засекречивания телеграфа представляла скорее техническую, чем теоретическую проблему, так как относительно небольшие скорости передачи легко могли быть реализованы на стандартном канале связи, а теория ручных шифров и машин предварительного шифрования создала хорошую базу для разработки линейного шифратора.

Засекречивание телефонной информации с её «аналоговой» формой требовало решения более сложных проблем, чем в случае с телеграфной информацией.

За начальную точку отсчета в развитии секретной телефонии следует принять 1930 г., когда под руководством молодого инженера Владимира Александровича Котельникова небольшая группа разработчиков – связистов создала новую аппаратуру, обеспечивающую засекречивание телеграфных и телефонных передач на коротковолновой линии связи.

Молодой В.А. Котельников, будущий вице-президент Академии наук, лауреат Ленинской и Государственных премий, председатель Верховного Совета РСФСР, дважды Герой Социалистического Труда, стал отцом секретной телефонии в нашей стране.

Чуть позднее, в 1931 г., в области секретной телефонии уже работало 7 организаций. Среди них НИИ Народного Комиссариата Почт и Телеграфа (НКПиТ), НИИИС Красной Армии НКО, завод им. Коминтерна, завод «Красная Заря», НИИ связи и телемеханики ВМФ, НИИ № 20 Народного Комиссариата Электротехнической Промышленности, подразделения НКВД. Еще позднее, в 1938 и 1939 гг. в ЦНИИ связи НКПиТ были организованы две лаборатории под руководством В.А. Котельникова по засекречиванию телеграфной и телефонной информации.

С началом Великой Отечественной войны сотрудники завода «Красная Заря» были эвакуированы в г. Уфа и входили в состав Государственного союзного производственно-экспериментального института (ГСПЭИ 56), где продолжала результативно работать. Лаборатория В.А. Котельникова была разделена на две части: основная часть с ним самим была эвакуирована в ГСПЭИ 56, а другая часть была передана в НКВД СССР.

В первые послевоенные годы коллектив специалистов, работавший в ГСПИ 56, был практически сформирован. Большинство сотрудников завода «Красная Заря» возвратились в г. Ленинград, сотрудники лаборатории В.А. Котельникова были переведены в отдел правительственной связи (ОПС) МГБ СССР, сам он стал работать в МЭИ.

Одновременно с созданием аппаратуры засекречивания были начаты работы по её дешифрованию. В 6 управлении МГБ была создана группа под руководством А.П. Петерсона, которая одновременно с работами по созданию аппаратуры шифрования занялась вопросами дешифрования. С середины 1944 г. группа А.П. Петерсона начала «сокрушать» одну аппаратуру за другой. В итоге в 28.12.1945 г. был составлен отчет, в котором постулировалось, что аналоговая аппаратура шифрования мозаичного типа теоретически дешифруема. В 1947 г. в лаборатории секретной телефонии ОПС МГБ группой под руководством К.Ф. Калачева было создано автоматическое устройство дешифрования вслед за разговором. В разработке аппаратуры засекречивания телефонии наступил кризис. Для того, чтобы получить недешифруемую аппаратуру засекречивания телефонных переговоров, речь необходимо сначала перевести в цифровую форму, а затем зашифровать. Было предложено использовать для этих целей вокодер. Руководство МГБ СССР, очевидно, понимало не только важность, но и сложность проблемы, возникшей в секретной телефонии. Необходимо было собрать всех имеющихся специалистов, обеспечить их всем необходимым и поручить создание аппаратуры с гарантией недешифруемости. Руководство МГБ решило поручить эту работу отделу оперативной техники (ОТТ) МГБ СССР.



Рис.1. Главный корпус Марфинской лаборатории

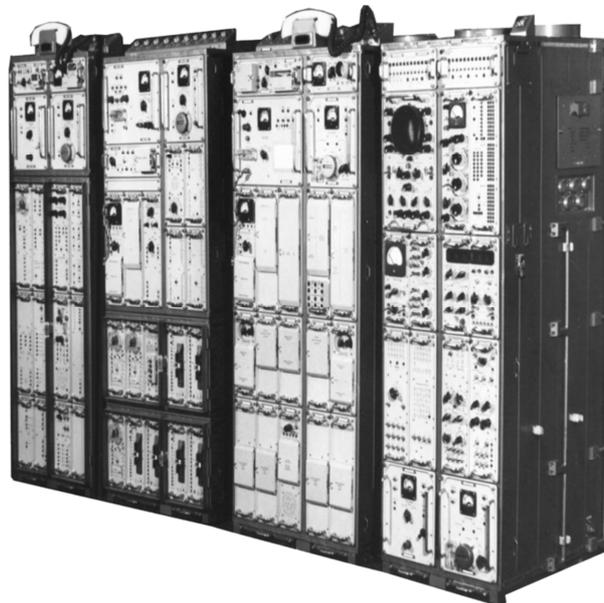


Рис.2. Аппаратура шифрования с гарантированной стойкостью телефонной информации и передачи её по каналам тональной частоты и коротковолновым каналам: год выпуска 1970; масса 1080 кг; потребляемая мощность 2,1 кВт

Было подготовлено постановление Совета Министров СССР, которое вышло 21 января 1948 г., в соответствии с которым в поселке Марфино под Москвой была организована спецлаборатория в составе ОТТ по разработке засекречивающей аппаратуры для ВЧ связи. В связи с тем, что ОТТ в своей работе использовал труд заключенных, это наложило свой отпечаток на работу спецлаборатории. Работа лаборатории, правда в достаточно негативном аспекте, отражена в книге А.И. Солженицына «В круге первом», Л.З. Копелева «Утоли мои печали» и наиболее объективно в книге К.Ф.Калачева «В круге третьем».

Использование труда заключенных было, конечно же, ошибкой, которая была исправлена через четыре года – постановлением Совмина СССР от 12.01.52 г. в Главном управлении Специальной Службы при ЦК ВКПб создается НИИ-2, ныне ФГУП «НИИ автоматики».

Работы по созданию аппаратуры шифрования начали проводиться все более широким фронтом в инте-

ресах правительственной связи, и, в том числе для Вооруженных Сил.

Первая серийная аппаратура засекреченной связи на новом предприятии была создана уже в 1954 году и установлена на самых протяженных в то время в мире линиях связи: Москва – Берлин, Москва – Пекин.

За прошедшие 60 лет коллективом «НИИ автоматики» создано несколько поколений технических средств и систем шифрованной связи. Это обеспечило решение многообразных задач засекреченной связи, боевого и государственного управления в стране.

За работы по созданию вышеуказанных средств и систем лауреатами Ленинских и Государственных премий стали 38 сотрудников института, более 400 человек награждены орденами и медалями.

В 1978 году за достижения и области науки и техники «НИИ автоматики» был награжден Орденом Ленина.

В 50–60 годы в НИИА было создано первое поколение отечественной шифраппаратуры на полупроводниковых и ферритовых элементах: М-803-5, «Лиана»,

«Алмаз», «Коралл», «Эльбрус», «Яхта», «Булава» и другие.

В 79-80 годах создаются специальные комплексы технических средств засекреченной связи и управления на базе микросхем малой и средней степени интеграции: «Кавказ», «Роса», «Интерьер».

Наряду с традиционным направлением засекречивания телефонии создается новый класс аппаратов по защите цифровой и телекодовой информации: «Стрекоза», «Лань», «Газель», «Грим», «Алибек», «Чегет», «Ветер», «Штиль», «Шторм», «Шквал», «Дуб», «Багет» и другие.

Разработка аппаратуры комплексов и систем засекреченной связи всегда опиралась на результаты фундаментальных теоретических исследований в области криптографии, проводимых институтом совместно с Институтом криптографии, связи и информатики, Академии криптографии РФ и ведущими академическими вузами страны.

С развитием информационных технологий появилась потребность в засекречивании передачи данных, факсимильной информации, видеоизображений, телеметрии и т.д. Со временем коллектив НИИ-2 стал «захлебываться» от возникающих новых задач. Для его разгрузки приказом Госкомитета по радиоэлектронике при СМ СССР от 18.01.1958 г. был создан НИИ-3. В настоящее время это ФГУП «Пензенский научно-исследовательский электротехнический институт», которому были поручены вопросы создания шифротехники для телекодовой и телеграфной информации в интересах различных заказчиков.

Новый всплеск активности по созданию образцов шифротехники пришелся на вторую половину 80-х годов прошлого столетия. Это связано с началом широкого применения персональных компьютеров и развитием компьютерных сетей. В настоящее время более 40 предприятий имеют лицензии на право разработки и изготовления шифротехники различного назначения.

Коллектив ФГУП «НИИ автоматика» по инициативе первого заместителя директора (с февраля 1999 г. - директора) С.А. Букашкина развертывает работы по освоению новой технологии проектирования аппаратуры на базе импортных процессоров цифровой обработки сигналов (DSP) фирмы Texas Instruments (США) и программируемых логических матриц фирмы Xilinx (США). Это происходит в условиях возросшей конкуренции и возрастаниям требований заказчиков к тактико-техническим характеристикам аппаратуры. Работа проводилась в тесном сотрудничестве с Научно-Исследовательским Центром (НИЦ) Федерального агентства правительственной связи и информации.

Результат не замедлил сказаться. В рекордные по старым меркам сроки удалось создать ряд принципиально новых изделий, которые по своим тактико-экономическим показателям намного превосходили предыдущее поколение шифротехники. К таким изделиям относится аппаратура Е-16, Е-9У, Е-11, «Медео» и особенно «Гамма». Демонстрация их на выставке «Связь-95» показала весьма большой интерес к ним со стороны ведущих зарубежных фирм, таких как Motorola, Siemens, NEC и многих других. Это свиде-

тельствует о том, что удалось в короткие сроки создать продукцию, во многом соответствующую мировому уровню.

В 1995 г. первый заместитель Генерального директора РГНПО «Автоматика» д.т.н., профессор, академик АК РФ, академик МАИ Букашкин С.А. делает доклад на секции №6 «Радиоэлектроника» НТС Госкомоборонпрома по вопросу: «О состоянии и перспективах развития техники защиты информации». НТС принимает решение: «Считать правильными и безальтернативными направления работ в РГНПО «Автоматика» по созданию перспективной техники защиты информации. Это реализовано на аппаратно-программных принципах с использованием современной высокоинтегрированной элементной базы отечественного и импортного производства, а также сетей специальной связи с использованием импортных компонентов (коммутаторы, терминальное оборудование и т.д.), так как только таким способом возможно быстрое создание специальных сетей связи современного по мировым оценкам уровня обслуживания».

Дальнейшее развитие событий показало правильность выбранного направления работ.

В 1998 году проходят государственные испытания аппаратов Е-16 (рис.3) и «Гамма» (рис 4).



Рис.3. Аппарат Е-16

Малогобаритный аппарат для автоматического шифрования речевой, факсимильной и документальной информации в сети подвижной радиосвязи в дуплексном режиме, передаваемой со скоростью 2,4/4, 8/9, 6 Кбит/с по УКВ и ТЧ каналам

Аппарат «Гамма-М» является стандартным телефонным аппаратом с интегрированным в него цифровым шифратором. Аппарат предназначен для шифрования телефонной, факсимильной и документальной информации в дуплексном режиме с гарантированной стойкостью.



Рис.4. Аппарат «Гамма-М»

Аппарат имеет три дуплексных режима связи: режим открытой связи (работает как стандартный телефонный аппарат); режим шифрования речи; режим

шифрования данных (факсимильные аппараты и ПЭВМ подключаются по стандартному интерфейсу V.24 / V.28 (RS-232-C)). Аппарат обеспечивает работу через телефонную коммутированную сеть общего пользования по 2-х проводной линии в соответствии с рекомендациями ITU-T V32bis.

В 2002 г. успешно завершаются государственные испытания системы радиоподвижной связи «Кавказ-9», в 2004 г. комплекса аппаратуры «Исполком» (рис. 5)

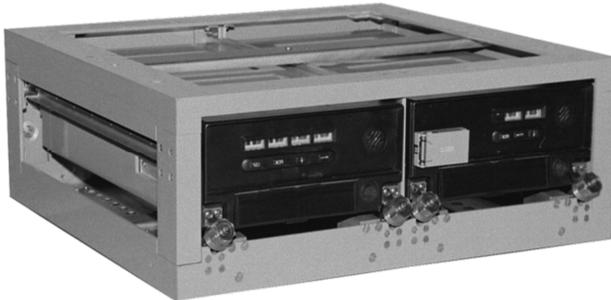


Рис.5. «Аппарат - 1И»

Основной многоканальный аппарат шифрования комплекса «Исполком» для сетей засекреченной связи силовых ведомств.

Обеспечивает шифрование информации на скоростях от 1,2 до 64 Кбит/с и образование от 1 до 42 основных шифрованных каналов на скорости 1,2 Кбит/с. Позволяет образовывать каналы шифрованной связи на скоростях от 2,4 до 32 Кбит/с в различных (программируемых) комбинациях

В 2006 году завершается модернизация аппарата Е-16. Результаты работы по реализации решения НТС Госкомоборонпрома 1995 года наглядно иллюстрируются рис. 6 «Эволюция». На рисунке приведены фотографии аппаратуры аналогичного назначения разработки 1979, 1998 и 2005 годов.

Изменения в подходах и принципах создания новой техники, а также требования рыночной экономики потребовали быстрой реализации программы технического перевооружения лабораторий и основных производственных участков, решения проблем кадрового обновления и структурных преобразования в институте.

Все это позволили только за последние годы разработать и передать в производство нескольких десятков образцов качественно новой аппаратуры. На базе новых технических средств, и полной мере соответствующих международным стандартам, созданы и введены в эксплуатацию защищенные сети и системы связи. Качественно новую технику получили Вооруженные силы России, представители других силовых структур.

Научно-техническая общественность и руководство ФГУП «НИИ автоматики» понимают, что в современных условиях, при усложняющихся информационно-телекоммуникационных технологиях, проблемы безопасности управления государством и Вооруженными Силами только путем создания аппаратуры шифрования решить невозможно. Проблема обеспечения безопасности – проблема комплексная и может решаться только комплексом мер при создании автоматизированных систем управления и систем связи. Именно

поэтому, по инициативе директора ФГУП «НИИ автоматики» в институте развернуты работы, напрямую не связанные с шифротехникой, но непосредственно касающиеся вопросов обеспечения безопасности в современных сетях связи и системах управления.

Современный этап развития общества характеризуется возрастающей ролью информационной сферы, которая, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации. Решения Президента Российской Федерации, Правительства Российской Федерации, направленные на ускоренное внедрение инновационных технологий в информационно-телекоммуникационное обеспечение деятельности органов государственной власти, обороны, безопасности и правопорядка, определяют значительный рост объемов обрабатываемой в технических средствах и передаваемой по каналам связи информации ограниченного доступа, в том числе, содержащей сведения, составляющие государственную тайну. Вместе с тем продолжает эксплуатироваться значительное количество ранее созданных ведомственных информационно-телекоммуникационных систем и автоматизированных систем управления в интересах обеспечения обороны, безопасности и правопорядка.

В соответствии с Концепцией национальной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 17 декабря 1997 г. № 1300, одной из важнейших задач являются защита государственного информационного ресурса, и, прежде всего, в федеральных органах государственной власти и на предприятиях оборонного комплекса. Основой для обеспечения гарантированной защиты информации является применение средств шифровальной техники, средств криптографической защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну.

На сегодня ФГУП «Научно-исследовательский институт автоматики» – головной исполнитель работ по одной из наиболее значимых Федеральных целевых программ Российской Федерации, направленной на создание и развитие информационно-телекоммуникационной системы специального назначения в интересах органов государственной власти.

Аппараты, комплексы средств шифрованной связи, защищенные сети и информационно-телекоммуникационной системы, разработанные и изготовленные в ФГУП «НИИА», установлены в Кремле, Доме Правительства, Государственной Думе, Счетной палате, Таможенном комитете, Центральном банке РФ, министерствах, пунктах управления ФСО, МО РФ. Они надежно работают на космических аппаратах, самолетах, кораблях, подводных лодках, автомобилях, бронетранспортерах и т.д.

Услугами правительственной связи пользуются должностные лица всех ветвей и уровней государственной власти. Рядом с Президентом Российской Федерации постоянно находится одно из изделий нашего института, известное всему миру как «ядерный чемоданчик».



Рис.6 «Эволюция»

В начале 90-х годов начали бурно развиваться телекоммуникационные технологии. Главным направлением развития стал переход на асинхронные сети связи с коммутацией пакетов. Стремительно развивается Интернет и связанные с ним технологии. Появляется новый класс сетей связи – мобильные сети связи. Стало ясно, что эра разработки отдельных шифровальных аппаратов закончилась – началась эра разработки криптозащищенных сетей связи, опирающихся на современные телекоммуникационные технологии.

Изменение технической политики потребовало привлечения молодых специалистов, владеющих современными технологиями систем связи и разработки РЭА. Имея в виду трудности привлечения талантливых молодых специалистов на работу в режимное предприятие Москвы, директор принял решение об организации филиалов ФГУП «НИИА» на базе Рязанского государственного радиотехнического университета и Санкт-Петербургского государственного университета. Решение оправдало себя: сотрудники филиалов принимают активное и плодотворное участие в новейших разработках.

В ФГУП «НИИА» работает базовая кафедра Московского института радиозлектроники и автоматики (технический университет МИРЭА), ведется подготовка аспирантов и докторантов.

За последнее пятилетие проведена коренная модернизация опытного производства. Установленные импортные станки и автоматические линии повышенной точности и производительности позволяют выпускать изделия, соответствующие современному мировому уровню.

Свое шестидесятилетие ФГУП «НИИА» встречает рядом успешных разработок. К ним относятся:

- высокоскоростной криптомаршрутизатор «Никель-4», позволяющий создавать защищенные сети для передачи всех видов информации;
- аппаратные машины современных полевых сетей связи «Переселенец-5» (аппаратные П-244И и П-242И);
- станции обеспечения безопасности различных криптозащищенных сетей связи;
- подсистема мобильной (сотовой) защищенной сети связи «Сапфир»;
- телефон шифрованной связи по сети Internet «Круз» и многое другое.

Разработан мобильный комплекс шифрованной связи для выездных мероприятий высшего руко-

водства страны, который вобрал в себя лучшие достижения шифраторостроения. Комплекс получил высокую оценку Президента РФ и сопровождает его во всех поездках по стране и за рубежом. На базе основного аппарата комплекса созданы десятки модификаций, предназначенных для организации прямых линий для связи с руководителями иностранных государств (аппарат Е-45). Аппарат протестирован специалистами США и рекомендован ими для оснащения прямой линии Москва – Вашингтон.

Не забывает ФГУП «НИИА» и о коммерческих потребителях. Большая часть коммерческих проектов сориентирована на массового потребителя, на их применимость в крупных корпоративных структурах. Более подробную информацию о коммерческой продукции можно найти на сайте по адресу <http://niia.ru/>

В целях сохранения и развития научно-производственного и технологического потенциала предприятий по производству систем и средств шифровальной техники, а также информационно-телекоммуникационных систем специального назначения в интересах обороноспособности, безопасности государства, Указом Президента РФ от 16.10.2010 г. № 1261 ФГУП «Научно-исследовательский институт автоматики» преобразуется в открытое акционерное общество «Концерн «Автоматика», 100% акций которого находится в федеральной собственности. В эту интегрированную структуру войдут, после преобразования в открытые акционерные общества, еще 7 предприятий: Башкирское ПО «Прогресс», завод «Калугаприбор», Калужский электромеханический завод, НПО «Сигнал» (г. С-Петербург), Пензенский научно-исследовательский Электротехнический институт, ПО «Электроприбор» (г. Пенза) и Уфимский завод микроразработки «Магнетрон».

Концентрация основных разработчиков и изготовителей шифротехники и оборудования телекоммуникационных систем специального назначения в единый комплекс даст, несомненно, новые возможности по ускорению разработки и освоению в производстве современных средств комплексной защиты информации в Вооруженных силах РФ, структурах государственной власти и ключевых отраслях экономики Российской Федерации.

Директор ФГУП «НИИ автоматики»,
академик Академии криптографии РФ,
д.т.н., профессор С.А. Букашкин